CLAIMS

WHAT IS CLAIMED IS:

1. A system, comprising:

a bus;

a memory coupled to the bus, wherein the memory includes a plurality of storage locations, wherein the plurality of storage locations are divided into a plurality of memory units; and

a device coupled to access the memory over the bus, wherein the device comprises:

one or more locks configured to control access to one or more of the plurality of memory units; and

an access lock override register that stores one or more access lock override bits, including a lock override bit;

wherein access to the one or more of the plurality of memory units is not allowed when the lock override bit is set.

2. The system of claim 1, wherein the bus is configured to operate according to an LPC bus protocol.

3. The system of claim 1, wherein the memory is a ROM.

4. The system of claim 3, wherein the ROM is a BIOS ROM.

5. The system of claim 1, wherein the device is a south bridge.

6. The system of claim 1, wherein the locks include a plurality of registers, wherein one or more entries in one or more of the plurality of registers indicate an access control setting for one or more of the memory units.

7. The system of claim 6, wherein at least one of the plurality of registers is configured to store three locking bits for one of the memory blocks, wherein the three locking bits include a read lock bit, a write lock bit, and a lock-down bit, wherein the read lock bit and the write lock bit are permanent until reset when the lock-down bit is set.

8. The system of claim 6, wherein at least one of the plurality of registers is configured to store eight bits, wherein the eight bits include three locking bits for one of the memory blocks and another three locking bits for another one of the memory blocks, wherein the three locking bits include a first read lock bit, a first write lock bit, and a first lock-down bit, wherein when the first lock-down bit is set, the first read lock bit and the first write lock bit are permanent until reset, and wherein the another three locking bits include a second read lock bit, a second write lock bit, and a second lock-down bit, wherein when the second lock-down bit is set, the second read lock bit and the second write lock bit are permanent until reset.

9. The system of claim 8, wherein the at least one of the plurality of registers is configured with bit 0 as the first write lock bit, bit 1 as the first lock-down bit, bit 2 as the first read lock bit, bit 4 as the second write lock bit, bit 5 as the second lock-down bit, and bit 6 as the first read lock bit.

10. The system of claim 1, wherein the one or more access lock override bits further include an change override lock bit that, when set, prevents the lock override bit from being changed.

11. The system of claim 10, wherein the change override lock bit is open at reset.

12. A method for operating a computer system, the method comprising:

requesting a memory transaction for one or more memory addresses;

determining a lock status for the one or more memory addresses;

returning the lock status for the one or more memory addresses;

if the lock status indicates that the memory transaction for the one or more memory addresses is not allowed, determining if the lock status for the one or more memory address can be changed;

if the lock status of the one or more memory addresses can be changed, changing the lock status of the one or more memory addresses to allow the memory transaction.

13. The method of claim 12, wherein determining a lock status includes reading a first lock bit; and wherein returning the lock status includes returning the value of the first lock bit.

14. The method of claim 13, wherein determining if the lock status for the one or more memory address can be changed includes reading a second lock bit.

15. The method of claim 14, wherein changing the lock status of the one or more memory addresses to allow the memory transaction includes changing the value of the first lock bit.

16. A system, comprising:

a processor;

a device coupled to the processor, wherein the device includes:

one or more sub-devices;

one or more access locks, wherein the one or more access locks are configured to prevent access to the one or more sub-devices when the one or more access locks are engaged; and

an access lock override register that stores one or more access lock override bits, including a lock override bit, wherein access to the one or more sub-devices is not allowed when the lock override bit is set.

17. The system of claim 16, wherein the device includes a bridge.

18. The system of claim 16, wherein the one or more sub-devices include one or more from the group consisting of:

a duration timer;

mailbox RAM;

a TCO counter;

a monotonic counter;

scratchpad RAM; and

a random number generator.

19. The system of claim 16, wherein the one or more access locks include a single access lock configured to prevent access to a plurality of the one or more sub-devices when the single access lock is engaged.

20. The system of claim 19, wherein the single access lock includes a sequester register configured to store a sequester bit.

21. The system of claim 16, wherein the one or more access locks include two or more access locks, wherein a first access lock is configured to prevent a first access to a plurality of the one or more sub-devices when the first access lock is engaged, and wherein a second access lock is configured to prevent a second access to a plurality of the one or more sub-devices when the second access lock is engaged.

22. The system of claim 21, wherein the first access is a read operation, and wherein the second access is a write operation.

23. The system of claim 16, wherein the one or more access locks include a plurality of sequester registers.

24. The system of claim 23, wherein each of the plurality of sequester registers is configured to prevent access to a different one of the one or more sub-devices when engaged.

25. The system of claim 24, wherein each of the plurality of sequester registers is configured to store one bit.

26. The system of claim 24, wherein each of the plurality of sequester registers is configured to store a plurality of bits.

27. The system of claim 26, wherein the one or more access lock override bits further include an change override lock bit that, when set, prevents the lock override bit from being changed.

28. The system of claim 27, wherein the change override lock bit is open at reset.

29. A method of operating a computer system in system management mode (SMM), the computer system including a processor coupled to security hardware, and to a first device, the method comprising:

processing SMM code instructions;

unlocking security hardware;

checking a lock status of the security hardware;

accessing a first device;

locking the security hardware;

setting a bit preventing changes to the locks of the security hardware; and

calling an SMM exit routine.

30. A system, comprising:

a processor configured to operate in an operating mode, wherein the operating mode is one of a plurality of operating modes including a secure operating mode;

one or more secured assets coupled to the processor; and

security hardware configured to control access to the secured assets dependant upon the operating mode of the processor, wherein the security hardware is configured to allow access to the secure assets in the secure operating mode, and wherein the security hardware includes a lock override register configured to deny access to the secure assets when a lock override bit is set.

31. The system of claim 30, wherein the secured assets comprise one or more of the group consisting of:

a random number generator,

a secure management register,

a monotonic counter, and

a secure memory.

32. The system of claim 30, wherein the security hardware comprises:

an initiation register, wherein an entry in the initiation register is an indication to change the operating mode of the processor to the secure mode.

33. The system of claim 30, wherein the secure operating mode comprises system management mode.

34. The system of claim 30, wherein the security hardware comprises:

a kick-out timer configured to provide an indication to the processor to exit the secure mode.

35. The system of claim 34, wherein the security hardware further comprises:

a re-initiation timer configured to provide an indication to the processor to enter the secure mode.

36. The system of claim 30, wherein the security hardware comprises:

a duration timer configured to operate while the processor is operating in the secure mode, wherein the duration timer is configured to provide an indication of how long the processor is in the secure mode.

37. The system of claim 36, wherein the security hardware comprises:

a kick-out timer configured to provide an indication to the processor to exit the secure mode.

38. The system of claim 37, wherein the kick-out timer and the duration timer comprise a single timer.

39. The system of claim 37, wherein the security hardware further comprises:

a re-initiation timer configured to provide an indication to the processor to re-enter the secure mode.

40. The system of claim 30, wherein the security hardware comprises:

mailbox RAM configured to store input and output data, wherein the mailbox RAM includes an inbox for storing input data for the one or more secured assets and an outbox for storing output data from the one or more secured assets.

41. The system of claim 40, wherein the input data for the one or more secured assets is addressed to the inbox of the mailbox RAM.

42. The system of claim 40, wherein the output data from the one or more secured assets is retrieved from an address at the outbox of the mailbox RAM.

43. The system of claim 40, wherein the security hardware further comprises:

access filters configured to provide input data or access requests to the inbox of the mailbox RAM if the processor is operating in the secure operating mode, wherein the access filters are further configured not to provide input data to the inbox of the mailbox RAM if the processor is not operating in the secure operating mode, and wherein the access filters are further configured to provide a predetermined response in lieu of data upon receipt of said access requests if the processor is not operating in the secure operating mode.

44. The system of claim 30, wherein the security hardware further comprises:

scratchpad RAM, wherein each of the one or more secured assets is configured to access the scratchpad RAM for the storage of data.

45. The system of claim 30, further comprising:

a memory for storing data, wherein the memory is coupled to the processor and the processor is configured to store and retrieve data from the memory in substantially all of the plurality of operating modes.

46. The system of claim 30, wherein the security hardware comprises:

access filters configured to provide access requests to one or more of the one or more secured assets when the processor is operating in the secure operating mode, wherein the access filters are further configured to provide a predetermined response in lieu of data if the processor is not operating in the secure operating mode.

47. The system of claim 46, wherein the security hardware further comprises:

access locks coupled to the access filters, wherein the access locks are configured to disable the access filters in an unlocked mode.

48. The system of claim 30, further comprising:

a battery, wherein the battery provides reserve power to the one or more secured assets.

49. The system of claim 30, further comprising:

a battery, wherein the battery provides reserve power to the security hardware.

50. A method for providing access to secured assets in a computer system, the method comprising:

operating the computer system in a first operating mode different from a secure operating mode;

restricting access to the secured assets in response to the computer system being in the first operating mode; and

determining if the secured assets would be accessible if the computer system were in the secure operating mode;

requesting access to the secured assets while in the first operating mode;

receiving access to the secured assets while in the first operating mode; and

permitting access to the secured assets in response to receiving access to the secured assets while in the first operating mode.

51. The method as set forth in claim 50, wherein the secured assets comprise a secure memory, and wherein permitting access to the secured assets comprises reading data from or writing data to the secure memory.

52. The method as set forth in claim 50, wherein the secured assets comprise a random number generator, and wherein permitting access to the secured assets comprises requesting a random number from the random number generator and receiving the random number from the random number generator.

53. The method as set forth in claim 50, wherein the secured assets comprise a monotonic counter, and wherein permitting access to the secured assets comprises requesting a value stored in the monotonic counter and receiving the value stored in the monotonic counter.

54. The method as set forth in claim 50, wherein permitting access to the secured assets comprises reading output data from or writing input data to a mailbox RAM from which the secure assets write the output data and read the input data.

55. The method as set forth in claim 50, further comprising:

receiving an access request for one of the secured assets;

receiving the access request to the secured assets while in the first operating mode; and

wherein restricting access to the secured assets further comprises responding with a predetermined response in lieu of data in response to receiving the access request for one of the secured assets, and in response to the access request to the secured assets while in the first operating mode being denied.

56. The method as set forth in claim 50, further comprising:

setting an access lock to an unlocked state; and

wherein permitting access to the secured assets further comprises overriding restricting access to the secured assets and providing the access request to a selected one of the secured assets in response to receiving the access request for the selected one of the secured assets and in response to setting the access lock to the unlocked state.

57. The method of claim 50, wherein determining if the secured assets would be accessible if the computer system were in the secure operating mode comprises determining if a lock is set to indicate that secured assets are accessible when in the secure operating mode.

58. A computer readable program storage device encoded with instructions that, when executed by a computer, performs a method of operating a computer system, the method comprising:

requesting a memory transaction for one or more memory addresses;

determining a lock status for the one or more memory addresses;

returning the lock status for the one or more memory addresses;

if the lock status indicates that the memory transaction for the one or more memory addresses is not allowed, determining if the lock status for the one or more memory address can be changed;

if the lock status of the one or more memory addresses can be changed, changing the lock status of the one or more memory addresses to allow the memory transaction.

59. The computer readable program storage device of claim 58, wherein determining a lock status includes reading a first lock bit; and wherein returning the lock status includes returning the value of the first lock bit.

60. The computer readable program storage device of claim 59, wherein determining if the lock status for the one or more memory address can be changed includes reading a second lock bit.

61. The computer readable program storage device of claim 60, wherein changing the lock status of the one or more memory addresses to allow the memory transaction includes changing the value of the first lock bit.

62. A computer readable program storage device encoded with instructions that, when executed by a computer system including a processor coupled to security hardware, and to a first device, performs a method of operating the computer system in system management mode (SMM), the method comprising:

processing SMM code instructions;

unlocking security hardware;

checking a lock status of the security hardware;

accessing a first device;

locking the security hardware;

setting a bit preventing changes to the locks of the security hardware; and

calling an SMM exit routine.

63. A computer readable program storage device encoded with instructions that, when executed by a computer system performs a method for providing access to secured assets in the computer system, the method comprising:

operating the computer system in a first operating mode different from a secure operating mode;

restricting access to the secured assets in response to the computer system being in the first operating mode; and

determining if the secured assets would be accessible if the computer system were in the secure operating mode;

requesting access to the secured assets while in the first operating mode;

receiving access to the secured assets while in the first operating mode; and

permitting access to the secured assets in response to receiving access to the secured assets while in the first operating mode.

64. The computer readable program storage device as set forth in claim 63, wherein the secured assets comprise a secure memory, and wherein permitting access to the secured assets comprises reading data from or writing data to the secure memory.

65. The computer readable program storage device as set forth in claim 63, wherein the secured assets comprise a random number generator, and wherein permitting access to the secured assets comprises requesting a random number from the random number generator and receiving the random number from the random number generator.

66. The computer readable program storage device as set forth in claim 63, wherein the secured assets comprise a monotonic counter, and wherein permitting access to the secured assets comprises requesting a value stored in the monotonic counter and receiving the value stored in the monotonic counter.

67. The computer readable program storage device as set forth in claim 63, wherein permitting access to the secured assets comprises reading output data from or writing input data to a mailbox RAM from which the secure assets write the output data and read the input data.

68. The computer readable program storage device as set forth in claim 63, the method further comprising:

receiving an access request for one of the secured assets;

receiving the access request to the secured assets while in the first operating mode; and

wherein restricting access to the secured assets further comprises responding with a predetermined response in lieu of data in response to receiving the access request for one of the secured assets, and in response to the access request to the secured assets while in the first operating mode being denied.

69. The method as set forth in claim 63, the method further comprising:

setting an access lock to an unlocked state; and

wherein permitting access to the secured assets further comprises overriding restricting access to the secured assets and providing the access request to a selected one of the secured assets in response to receiving the access request for the selected one of the secured assets and in response to setting the access lock to the unlocked state.

70. The method of claim 63, wherein determining if the secured assets would be accessible if the computer system were in the secure operating mode comprises determining if a lock is set to indicate that secured assets are accessible when in the secure operating mode.